Christopher Springer (291180)
KELLER ROHRBACK L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497
cspringer@kellerrohrback.com

Lynn Lincoln Sarko, *pro hac vice forthcoming*
Gretchen Freeman Cappio, *pro hac vice forthcoming*
Cari Campen Laufenberg, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com
claufenberg@kellerrohrback.com

Attorneys for Plaintiff
Additional Attorneys Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

SUZIE HASLINGER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FACEBOOK, INC., CAMBRIDGE ANALYTICA LLC, and DOES 1-100,

Defendants.

No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Judge:

Table of Contents

I. INTRODUCTION

Plaintiff, Suzie Haslinger, individually and on behalf of herself and all others similarly situated ("Class Members"), files this Class Action Complaint against Facebook, Inc. ("Facebook" or the "Company"), Cambridge Analytica LLC ("Cambridge Analytica"), and Does 1-100 ("Doe Defendants") (collectively, "Defendants"), and alleges as follows based on personal knowledge, the investigation of her counsel, and information and belief:

II. NATURE OF THE ACTION

1. Facebook's 2.2 billion active users were recently shocked to learn that the social networking company had allowed Cambridge Analytica, as well as other, as yet unidentified entities, to obtain at least 50 million Facebook users' highly sensitive personal information for political marketing purposes, without their authorization. This personal information includes users' names, birthdates, hometowns, addresses, locations, interests, relationships, email addresses, photos, and videos, and is referred to herein as "Personal Information."

2. Whereas the Personal Information of Plaintiff and millions of other users was supposed to be protected and used only for disclosed and limited purposes, Cambridge Analytica—as well as other, as yet unidentified entities—without authorization, or exceeding any limited authorization they or their agents may have had, improperly collected this Personal Information and used it for their commercial benefit.

3. Facebook knew or should have known that this improper collection and use of its users' data was occurring, but failed to stop it and willfully ignored and failed to investigate the activities of Cambridge Analytica and other entities.

4. Even worse, Facebook was on notice of this misuse by at least 2015, when a whistleblower came forward. But, in further breach of its users' trust, Facebook failed to notify users until the misuse became public on account of various investigative media reports in March 2018.

5. Plaintiff is a victim of Defendants' breach of her privacy and other harms, who brings this proposed class action lawsuit on behalf of herself and all other persons who registered for Facebook accounts and whose Personal Information was obtained from Facebook by Cambridge Analytica or other entities without their authorization or in excess of their authorization.

III. JURISDICTION AND VENUE

6. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA") and 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5 million, exclusive of interests and costs, there are more than 100 members of the class, and at least one class member is a citizen of a state different from one or more Defendants.

7. Venue is proper under 28 U.S.C. § 1391(c), because Facebook resides in this district, and Defendants are corporations that do business in and are subject to personal jurisdiction in this district. Venue is also appropriate in this district, because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in or emanated from this district.

IV. PARTIES

A. Plaintiff

8. Plaintiff Suzie Haslinger is a citizen and resident of Virginia. Plaintiff has held a Facebook account for approximately ten years.

B. Defendants

9. Facebook, Inc., a publicly traded company, is incorporated in Delaware. The Company's principal executive offices are located at 1601 Willow Road, Menlo Park, California 94025. Pursuant to 28 U.S.C. § 1332, Facebook is a citizen of Delaware and California.

10. Facebook builds and operates various products designed for people who want to connect and communicate with one another through electronic devices, including mobile devices and personal computers. The Company trades on NASDAQ under the ticker symbol "FB."

11. Facebook operates a social networking website that "enables people to connect, share, discover, and communicate with each other on mobile devices and personal computers."[1] This website allows users to share information, photographs, website links, and videos. Through this website and its other products, Facebook enables its roughly 2.2 billion monthly active users to "engage with [other] people on Facebook" in a variety of ways, "the most important of which is [the] News Feed which displays an algorithmically-ranked series of stories and advertisements individualized for each person."[2]

[1] Facebook, Inc., Annual Report (Form 10-K) (Feb. 1, 2018) at 5.
[2] *Id.* at 5, 34.

12. On information and belief, Cambridge Analytica LLC is a Delaware limited liability company that is owned and operated by SCL Group. Cambridge Analytica maintains offices in New York and Washington, D.C. Cambridge Analytica "uses data to change audience behavior." Its business is focused on two divisions, data-driven marketing ("CA Commercial"), and data-driven campaigns ("CA Political"). CA Political's data-driven campaigns combine data mining and data analysis in such a manner as to enable Cambridge Analytica to "find your voters and move them to action."

13. Plaintiff does not know the true names of Defendants Does 1 through 100, inclusive, and therefore sues them by those fictitious names. Plaintiff is informed and believes, and on the basis of that information and belief alleges, that each of those defendants was proximately responsible for the events and happenings alleged in this complaint and for Plaintiff's injuries and damages.

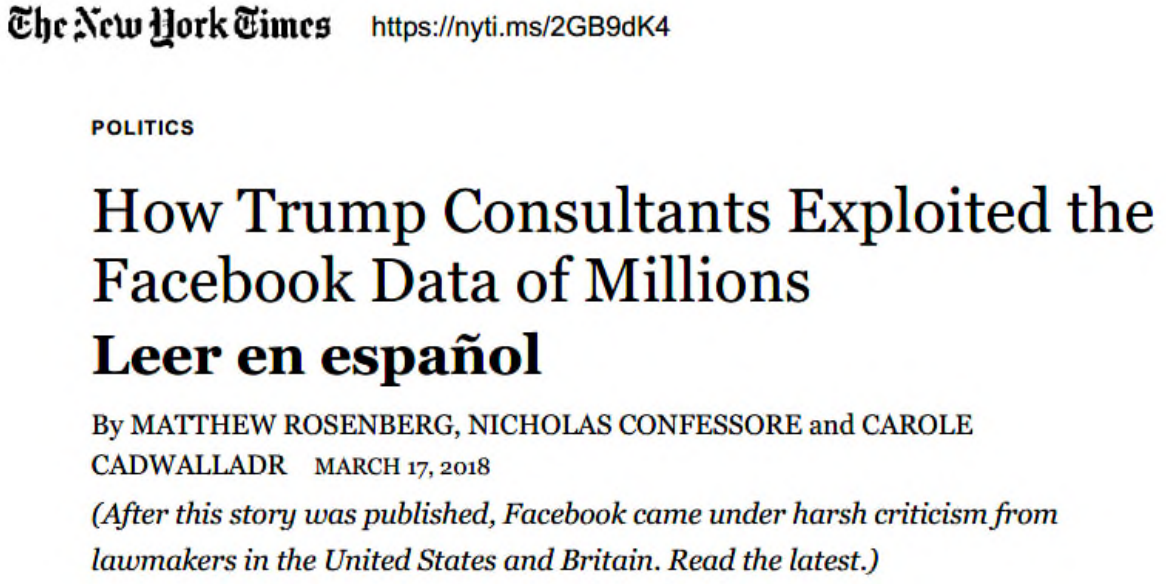
V. FACTUAL BACKGROUND

14. On March 17, 2018, both the *New York Times* and *The Guardian* reported that Cambridge Analytica had obtained Facebook users' Personal Information from Facebook, without the users' permission ("Data Breach").[3] The reports revealed that Cambridge Analytica used the data of 50 million people obtained from Facebook for political purposes, without proper disclosures or permission. The *New York Times* report stated:

> [T]he firm harvested private information from the Facebook profiles of more than 50 million users without their permission, according to former Cambridge employees, associates and documents, making it one of the largest data leaks in the social network's history. The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016.
>
> ***
>
> **But the full scale of the data leak involving Americans has not been previously disclosed — and Facebook, until now, has not acknowledged it.** Interviews with a half-dozen former employees and contractors, and a review of the firm's emails and

[3] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (emphasis added); *see also* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

documents, have revealed that Cambridge not only relied on the private Facebook data but still possesses most or all of the trove.[4]



The New York Times https://nyti.ms/2GB9dK4

POLITICS

How Trump Consultants Exploited the Facebook Data of Millions

Leer en español

By MATTHEW ROSENBERG, NICHOLAS CONFESSORE and CAROLE CADWALLADR MARCH 17, 2018

(After this story was published, Facebook came under harsh criticism from lawmakers in the United States and Britain. Read the latest.)

15. Facebook had assured its users that their "trust is important to us." The Company's Data Use Policy states: "we don't share information we receive about you with others unless we have . . . received your permission; given you notice such as by telling you about this policy; or removed your name and any other personally identifying information from it."[5]

16. On March 16, 2018, Facebook announced that it was suspending Cambridge Analytica and SCL Group from Facebook.[6] The Company stated that, in 2015, it learned it had been lied to by Dr. Aleksandr Kogan, a psychology professor at the University of Cambridge, and that Dr. Kogan had violated Facebook's "Platform Policies by passing data from an app that was using Facebook Login to SCL/Cambridge Analytica[.]"[7]

17. In 2013, Dr. Kogan reportedly requested and gained access to the personal information of approximately 300,000 Facebook users, after they downloaded the personality quiz application ("app")

---

[4] Rosenberg, Confessore & Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*.

[5] Data Use Policy (Nov. 15, 2013), https://www.facebook.com/full_data_use_policy (on information and belief, the Data Use Policy was available on this website until Mar. 22, 2018).

[6] Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, Facebook Newsroom (Mar. 16, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

[7] *Id.*

he designed, "MyDigitalLife" (also known as "thisisyourdigitallife") (collectively, "MyDigitalLife").[8] Facebook users were led to believe that psychologists would use the information collected from the app and would help them have a better understanding of their own personalities.

18. However, in addition to the personal data of the approximately 300,000 Facebook users that downloaded MyDigitalLife, Cambridge Analytica was able to gain access to the personal data of all of these users' Facebook "friends" as well—more than 50 million additional people who, according to Facebook, "had their privacy settings set to allow it."[9]

19. According to the March 20, 2018 article in *Forbes*, Christopher Wylie, a former Cambridge Analytica contractor, revealed in a recent interview with *The Guardian* how the data mining process at Cambridge Analytica worked: "With their profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages."[10]

20. Mr. Wylie also revealed that he had various documents that "showed how, between June and August 2014, the profiles of more than 50 million Facebook users had been harvested."[11] According to Mr. Wylie, Facebook users' profiles "contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles."[12]

21. Cambridge Analytica was thus implementing a psychological propaganda campaign on millions of Facebook users, without their knowledge or consent. Of the 50 million Facebook users affected by this scheme, only approximately 300,000 of them had downloaded the MyDigitalLife app—and, even then, they had agreed to share only their own personal information for the limited purposes

---

[8] *See* Mark Zuckerberg ("Zuckerberg Facebook Post"), Facebook (Mar. 21, 2018 12:36 PM), https://www.facebook.com/zuck/posts/10104712037900071; *see also* Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*.

[9] Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*.

[10] Parmy Olson, *Face-to-Face With Cambridge Analytica's Elusive Alexander Nix*, Forbes (Mar. 20, 2018), https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/.

[11] Carole Cadwalladr, *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, The Guardian (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[12] Rosenberg, Confessore & Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*.

associated with the app. Mr. Wylie stated: "Facebook data . . . was 'the saving grace' that let his team deliver the models it had promised[.]"[13]

22. On March 20, 2018, *The Guardian* reported that, according to Sandy Parakilas—a former Facebook insider who worked as a platforms operations manager and whose duties between 2011 and 2012 included "policing data breaches by third party software developers"—"Hundreds of millions of Facebook users are likely to have had their private information harvested by companies that exploited the same terms as the firm that collected data and passed it on to [Cambridge Analytica]."[14]


The Guardian

'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine

Sandy Parakilas says numerous companies deployed these techniques - likely affecting hundreds of millions of users - and that Facebook looked the other way

23. Mr. Parakilas stated that he warned senior executives at the Company that, due to its lackadaisical approach to data protection, the Company was at risk for a major data breach. He told *The Guardian* that: "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so [Facebook] had no idea what developers were doing with the data[.]" Mr. Parakilas also asserted that Facebook "did not use enforcement mechanisms, including audits of external developers, to ensure data was not being misused."[15]

24. Mr. Parakilas stated that an executive at Facebook "advised him against looking too deeply at how the data was being used." According to Mr. Parakilas, "[Facebook] felt that it was better

[13] *Id.*

[14] Paul Lewis, *'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine*, The Guardian (Mar. 20, 2018), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[15] *Id.*

not to know."[16]

25. Nonetheless, Facebook's lackadaisical approach to data protection continued after Mr. Parakila departed the Company, as evidenced by Cambridge Analytica's subsequent collection of the personal data of more than 50 million Facebook users without their authorization as well as the € 150,000 fine assessed by France's Commission on Informatics and Liberty ("CNIL") for "failing to prevent [Facebook] users' data being accessed by advertisers."[17] Facebook's assertion that "[p]rotecting people's information is at the heart of everything we do,"[18] rings hollow, particularly in light of Facebook founder and CEO Mark Zuckerberg's revelations:

> In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today.
>
> In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications.
>
> Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened.[19]

26. On March 20, 2018, *Bloomberg* reported that the Federal Trade Commission ("FTC") is "probing whether Facebook violated terms of a 2011 consent decree of its handling of user data that was transferred to [Cambridge Analytica] without users' knowledge."[20] As a result of the 2011 settlement

---

[16] *Id.*

[17] *See* Sudip Kar-Gupta & Mathieu Rosemain, *Facebook fined 150,000 euros by French data watchdog*, Reuters (May 16, 2017), https://www.reuters.com/article/us-facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUSKCN18C10C.

[18] Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook.*

[19] Zuckerberg Facebook Post.

[20] David McLaughlin, Ben Brody & Billy House, *Facebook Draws Scrutiny from FTC, Congressional Committees*, Bloomberg (Mar. 20, 2018), https://www.bloomberg.com/news/articles/2018-03-20/ftc-said-to-be-probing-facebook-for-use-of-personal-data.

with the FTC, Facebook "agreed to get user consent for certain changes to privacy settings as part of a settlement of federal chargers that is deceived consumers and forced them to share more personal information than they intended."[21] Additionally, "if the FTC finds Facebook violated terms of the consent decree, it has the power to fine the company more than $40,000 a day per violation."[22]

FEDERAL TRADE COMMISSION

Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices

27. Additionally, on March 20, 2018, various new agencies reported that the U.K. Parliament had summoned Mr. Zuckerberg to give evidence related to the Cambridge Analytica scandal. The U.K. House of Commons Digital, Culture, Media and Sport Committee stated: "Facebook previously gave evidence to the inquiry in Washington DC on [February 8]. However, Facebook has since failed to supply requested supplementary evidence to the Committee by the deadline of [March] 14th. Subsequent information about Facebook's connection to [Cambridge Analytica] raises further questions[.]"[23] The British lawmakers requested to "hear from a senior Facebook executive with the sufficient authority to give an accurate account of this catastrophic failure of process."[24]

28. Facebook's initial responses included the Zuckerberg Facebook Post as well as a

---

[21] *Id.*

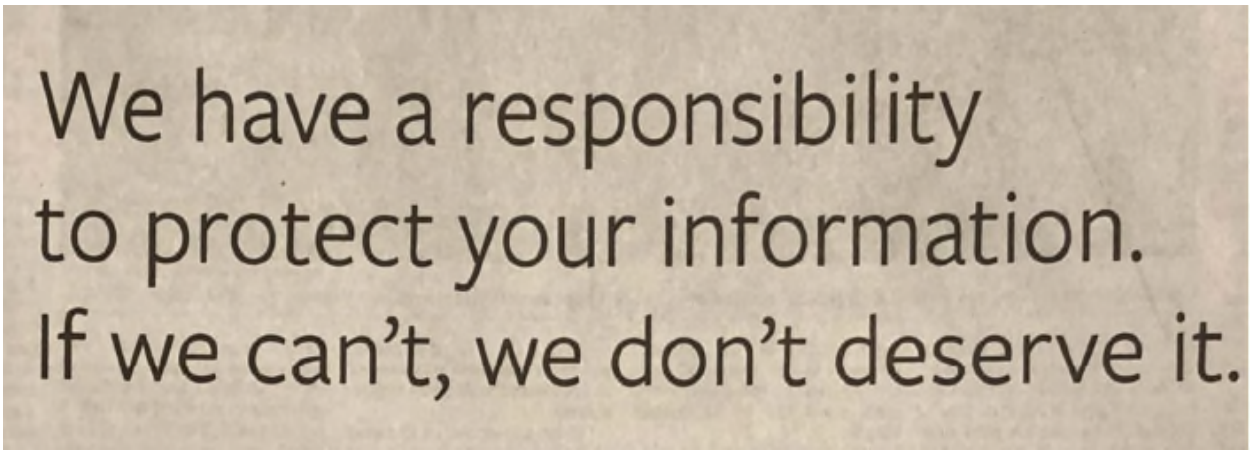
[22] On March 26, 2018, the Acting Director of the FTC, Tom Pahl, issued a formal statement regarding privacy and data security at Facebook, in which he confirmed that that the FTC "has an open non-public investigation into [Facebook's] practices." *See Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices*, FTC (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[23] Jill Lawless, *Facebook's Zuckerberg comes under fire from UK, US lawmakers*, Associated Press (Mar. 19, 2018), https://www.mysanantonio.com/business/technology/article/UK-lawmaker-says-Facebook-misled-Parliament-over-12762179.php.

[24] *Id.*

Facebook post on March 21, 2018 by Sheryl Sandberg, Facebook's Chief Operating Officer.[25] Ms. Sandberg acknowledged that Facebook is aware that "this was a major violation of people's trust" and expressed "regret that [Facebook] didn't do enough to deal with it."[26] Ms. Sandberg also stated that the Company is investigating "all apps that had access to large amounts of information before [Facebook] changed [its] platform in 2014 to dramatically reduce data access."[27]

29. On March 25, 2018, Facebook's CEO Mark Zuckerberg took out full-page ads in multiple British and American newspapers, in which he apologized for the "breach of trust" related to "leaked Facebook data of millions of people in 2014."[28] Mr. Zuckerberg also stated that he was "sorry [Facebook] didn't do more at the time," and assured Facebook users that Facebook is "now taking steps to ensure this doesn't happen again."[29]



30. On information and belief, Facebook maintained a Data Use Policy on its website until March 22, 2018. The Data Use Policy informed Facebook users of the following:

> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.

---

[25] *See* Sheryl Sandberg ("Sandberg Facebook Post"), Facebook (Mar. 21, 2018 12:40 PM), https://www.facebook.com/sheryl/posts/10160055807270177 (sharing Zuckerberg Facebook Post).
[26] *Id.*
[27] *Id.*
[28] Sheena McKenzie, *Facebook's Mark Zuckerberg says sorry in full-page newspaper ads*, CNN (Mar. 25, 2018), https://www.cnn.com/2018/03/25/europe/facebook-zuckerberg-cambridge-analytica-sorry-ads-newspapers-intl/index.html.
[29] *Id.*

> While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:
>
> - received your permission;
> - given you notice, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying information from it.

See Data Use Policy.

31. Ms. Sandberg noted that Facebook is "taking steps to reduce the data [Facebook users] give an app" when they use their Facebook account, and the Company intends to "make it easier" for users to have a better understanding of which apps they have "allowed to access [their] data."[30] Mr. Zuckerberg also informed Facebook users that the Company is "also investigating every single app that had access to large amounts of data before [Facebook] fixed this," because "[w]e expect there are others."[31]

32. Despite its knowledge that Class Members' Personal Information had been collected and used without their authorization, and that such misuse of Class Members' data presented substantial risk of further misuse, fraud, and other identity theft to Class Members, Facebook failed to provide notification to Class Members of the misuse of their Personal Information without and/or in excess of authorization, until March 2018—approximately three years after it was informed of the Data Breach.

33. Facebook's failure to notify Plaintiff and Class Members of the Data Breach was in violation of its data breach notification obligations under state laws including, *inter alia*, the California Customer Records Act, Cal. Civ. Code § 1798.80, et seq.

34. In the intervening years between 2015, when *The Guardian* notified Facebook of the Data Breach, and when Facebook admitted to Plaintiff and Class Members that this had occurred—only after subsequent reporting by *The New York Times* and *The Guardian*—Facebook failed to provide Plaintiff and Class Members with information that their sensitive information had been used without and/or in excess of their authorization and denied them the opportunity to take steps to protect themselves and mitigate their heightened risk of identity theft and other harms.

---

[30] *See* Sandberg Facebook Post.

[31] McKenzie, *Facebook's Mark Zuckerberg says sorry in full-page newspaper ads*.

35. As such, Plaintiff and Class Members were blindsided when they learned that their Personal Information had been accessed without and/or in excess of their authorization, and was allegedly used by Cambridge Analytica to create targeted advertising on behalf of President Trump's 2016 campaign.

VI. CLASS ACTION ALLEGATIONS

36. Pursuant to Rule 23(b)(2), 23 (b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure, Plaintiff brings her claims on behalf of a proposed nationwide class, defined as follows:

> All natural persons in the United States who registered for Facebook accounts and whose Personal Information was obtained from Facebook by Cambridge Analytica or other entities without authorization or in excess of authorization.

37. Excluded from the Class are Defendants and their parents, subsidiaries, affiliate, officers and directors, current or former employees, and any entity in which Facebook has a controlling interest, as well as the Court and its personnel presiding over this action.

38. Numerosity. The proposed Class is sufficiently numerous, as there are, upon information and belief, at least 50 million Class Members, and they are dispersed throughout the United States, making joinder of all members impracticable. Class Members can be readily identified and ascertained through the records maintained by Defendants.

39. Commonality. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

(a) Whether Facebook represented that it would safeguard the privacy of Plaintiff's and Class Members' Personal Information and not disclose it without consent;

(b) Whether Cambridge Analytica improperly obtained Plaintiff's and Class Members' Personal Information without authorization or in excess of authorization;

(c) Whether Facebook was aware of Cambridge Analytica's improper collection of Plaintiff's and Class Members' Personal Information;

(d) Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

(e) Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

(f) Whether Class Members' Personal Information was obtained by Cambridge Analytica and/or Doe Defendants;

(g) Whether Defendants' conduct violated the Federal Wiretap Act, 18 U.S.C. §§ 2501, et seq.;

(h) Whether Defendants' conduct violated the Stored Communications Act, 18 U.S.C. §§ 2701, et seq.;

(i) Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, et seq.;

(j) Whether Class Members are entitled to actual damages, statutory damages, and/or punitive damages; and

(k) Whether Class Members are entitled to injunctive relief.

40. **Typicality.** Plaintiff's claims are typical of the claims of the members of the proposed Class because, among other things, Plaintiff and Class Members sustained similar injuries as a result of Defendants' substantially uniform wrongful conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. Likewise, Plaintiff's legal claims all arise from the same operative facts and are based on the same legal theories.

41. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed Class. Plaintiff's interests do not conflict with Class Members' interests, and she has retained counsel experienced in complex class action and complex class action and privacy litigation to prosecute this case on behalf of the Class.

42. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class Members, and a class action is superior

to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

43. **Rule 23(b)(2).** Plaintiff also satisfies the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

44. **Rule 23(c)(4).** This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class Members involve particular issues that are common to all Class Members and capable of class wide resolution that will significantly advance the litigation.

VII. CAUSES OF ACTION

COUNT I — VIOLATION OF THE FEDERAL WIRETAP ACT, TITLE I OF THE ECPA (18 U.S.C. § 2510, et seq.) (Against All Defendants)

45. Plaintiff incorporates each and every allegation above as if fully set forth herein.

46. Plaintiff, individually, and on behalf of Class Members, asserts violations of 18 U.S.C. §§ 2511(1)(a), (1)(b), and (1)(d).

47. The Federal Wiretap Act, Title I of the Electronic Communications Privacy Act (the "Wiretap Act" or the "Act") prohibits the intentional interception by any person of the content of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

48. Section 2511(a) of the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . ."

49. Section 2511(1)(b) of the Wiretap Act provides a private right of action against any

person who:

> . . . intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
>
> (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
>
> (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
>
> (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
>
> (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
>
> (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States; . . . .

50. Section 2511(1)(d) of the Wiretap Act provides a private right of action against any person who:

> . . . intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of the subsection . . . .

51. Section 2502(a) of the Wiretap Act authorizes that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."

52. Section 2502(b) of the Wiretap Act provides that appropriate relief for violations under this section includes:

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorneys' fee and other litigation costs reasonably incurred.

53. Section 2502(c)(2) of the Wiretap Act provides that a court may assess damages for any violation under the section as follows:

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is greater of $100 a day for each day of violation or $10,000.

54. Plaintiff's use of Facebook to convey and store Personal Information, and the transmission of that Personal Information to and from Plaintiff's Facebook account, is considered "electronic communications" within the meaning of the Act. 18 U.S.C. § 2510(12).

55. Facebook, Cambridge Analytica, and Doe Defendants are each considered a "person" within the meaning of the Act. 18 U.S.C. § 2510(6).

56. Defendants used one or more devices comprising an "electronic, mechanical or other device or apparatus" within the meaning of the Act, 18 U.S.C. § 2510(5), to unlawfully acquire the contents of Plaintiff's Personal Information stored in and transmitted to and from Plaintiff's Facebook account.

57. Facebook knowingly and purposefully "intercepted" or "endeavored to intercept" Plaintiff's electronic communications in transit to and from Plaintiff's Facebook account and provided those communications to Cambridge Analytica and Doe Defendants without obtaining actual consent from any authorized party within the meaning of the Act. 18 U.S.C. § 2510(4). Likewise, Facebook intentionally used, or endeavored to use, the contents of Plaintiff's communications, knowing or having reason to know that the information was obtained through the interception of electronic communications.

58. Cambridge Analytica and Doe Defendants knowingly and purposefully "intercepted" or "endeavored to intercept" Plaintiff's Personal Information in transit to and from Plaintiff's Facebook account without obtaining actual consent from any authorized party within the meaning of the Act. *See* 18 U.S.C. § 2510(4). Likewise, Cambridge Analytica and Doe Defendants intentionally used, or endeavored to use, the contents of Plaintiff's communications, knowing or having reason to know that the information was obtained through the interception of electronic communications.

59. On information and belief, Facebook unlawfully intercepted, or endeavored to intercept, the content of these communications for the purpose of generating profit from Cambridge Analytica and Doe Defendants. This conduct was not performed by any employees within the ordinary course of Facebook's business and is not an instrumental part of Facebook's operation or incidental to the operation of Facebook or the provision of Facebook's electronic communication services, nor is it for the protection of Facebook's rights or property.

60. On information and belief, Cambridge Analytica and Doe Defendants unlawfully intercepted, or endeavored to intercept, the content of these communications for the purpose of generating profit. This conduct was not performed by any employees of Cambridge Analytica or Doe Defendants engaged in any activity necessary for the rendition of their respective electronic communication services nor for the protection of their respective rights or property nor the rights or property of Facebook.

61. As a result of Defendants' violations of the Act, Plaintiff and Class Members have suffered injury, which includes, but is not limited to, knowing and reckless impermissible interception and misuse of their electronic communications made to and from their Facebook accounts by Defendants in violation of the Act. Pursuant to the Act, Plaintiff and Class Members are entitled to statutory damages, actual damages, punitive damages, reasonable attorney's fees and litigation costs, as well as declaratory and injunctive relief.

COUNT II — VIOLATION OF THE STORED COMMUNICATIONS ACT, TITLE II OF THE ECPA (18 U.S.C. § 2701, et seq.)
(Against All Defendants)

62. Plaintiff incorporates each and every allegation above as if fully set forth herein.

63. Plaintiff, individually, and on behalf of Class Members, asserts violations of 18 U.S.C. § 2702.

64. The Stored Communications Act ("SCA") prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic communications service is provided and thereby obtaining an electronic communication while it is in "electronic storage." 18 U.S.C. §§ 2701(a) and 2702(a).

65. Section 2701(a)(1) of the SCA authorizes a private right of action against any person who

"intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains . . . access to wire or electronic communication while it is in electronic storage in such system . . . ."

66. Section 2701(a)(2) of the SCA authorizes a private right of action against any person who "intentionally exceeds an authorization to access [a facility through which an electronic communication service is provided] . . . and thereby obtains . . . access to wire or electronic communication while it is in electronic storage in such system . . . ."

67. Section 2702(a) of the SCA provides:

> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service;
>
> > (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
> >
> > (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; . . . .

68. Section 2707(b) of the SCA provides that Plaintiff and Class Members are entitled to:

> (1) such preliminary and other equitable or declaratory relief as may be appropriate;
>
> (2) damages under subsection (c); and
>
> (3) a reasonable attorneys' fee and other litigation costs reasonably incurred.

69. Section 2707(c) of the SCA provides that:

> . . . a court may assess damages suffered by the plaintiff and any profits made by the violators as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or

> intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

70. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

71. Facebook, Cambridge Analytica, and Doe Defendants are each considered a "person" within the meaning of the SCA. 18 U.S.C. § 2510(6).

72. Facebook, Cambridge Analytica, and Doe Defendants each provide "electronic communication service" within the meaning of the SCA. 18 U.S.C. § 2510(15)

73. Plaintiff's use of Facebook to convey and store Personal Information and transmission of that Personal Information to and from Plaintiff's Facebook account is considered "electronic communications" within the meaning of the Act. 18 U.S.C. § 2510(12).

74. The servers Defendants use to provide their respective electronic communications services to Plaintiff and Class Members are a "facility" within the meaning of the SCA.

75. Defendants intentionally accessed without authorization or, alternatively, intentionally exceeded authorization to access, Plaintiff's and Class Members' stored electronic communications, which contained highly sensitive Personal Information.

76. Facebook knowingly divulged Plaintiff's and Class Members' stored electronic communications to Cambridge Analytica and Doe Defendants, which contained highly sensitive Personal Information.

77. As a result of Defendants' violations of the SCA, Plaintiff and Class Members have suffered injury, which includes, but is not limited to, Defendants' intentionally accessing Plaintiff's and Class Members' stored electronic communications without (or in excess of) authorization and by Defendant Facebook's divulging to Cambridge and Doe Defendants the contents of Plaintiff's and Class Members' stored electronic communications, which contained sensitive Personal Information.

78. Pursuant to the Act, Plaintiff and Class Members are entitled to statutory damages, actual

damages, reasonable attorney's fees and litigation costs, as well as declaratory and injunctive relief.

COUNT III — NEGLIGENCE
(Against Defendant Facebook)

79. Plaintiff incorporates each and every allegation above as if fully set forth herein.

80. Facebook owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding their sensitive Personal Information, including protecting it from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties without or in excess of authorization provided. This duty included Facebook ensuring that no third-party apps, including the MyDigitalLife app, were improperly collecting, storing, and/or obtaining Plaintiff's and Class Members' Personal Information.

81. Facebook knew Plaintiff and Class Members consider their Personal Information to be sensitive and valuable, and that Plaintiff and Class Members had entrusted Facebook to safeguard their Personal Information.

82. Facebook acknowledged in its Data Use Policy that it had a duty to adequately protect Class Members' Personal Information.

83. Facebook had a special relationship with Plaintiff and Class Members as a result of being entrusted with their Personal Information, which provided an independent duty of care. Plaintiff's and Class Members' willingness to entrust Facebook with their Personal Information was predicated on the understanding that Facebook would take appropriate measures to protect it. Moreover, Facebook was capable of protecting Plaintiff and Class Members' Personal Information.

84. Facebook owed a duty to timely disclose to Plaintiff and Class Members that Facebook had allowed their Personal Information to be accessed by Cambridge and Doe Defendants without Class Members' authorization. Plaintiff and Class Members had a reasonable expectation that Facebook would inform them of any misuse of their Personal Information in a timely manner.

85. Facebook breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard and prevent impermissible disclosure of Plaintiff's and Class Members' Personal Information; (b) failing to disclose that its data security practices were inadequate to safeguard and prevent impermissible disclosure of Plaintiff's and Class Members' Personal Information; and (c) failing to provide adequate and timely notice that Plaintiff's

and Class Members' Personal Information had been improperly obtained by Cambridge Analytica and Doe Defendants.

86. But for Facebook's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information would not have been impermissibly disclosed to unauthorized parties, which resulted in misuse of Plaintiff's and Class Members' Personal Information.

87. Plaintiff and Class Members were foreseeable victims of Facebook's inadequate data security practices. Facebook knew or should have known that allowing unauthorized parties to access Plaintiff's and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

88. As a result of Facebook's negligent failure to safeguard Plaintiff's and Class Members' Personal Information, Plaintiff and Class Members have suffered injury, which includes but is not limited to impermissible disclosure of their Personal Information, both directly and indirectly by Facebook, and exposure to a heightened, imminent risk of misuse, fraud, identity theft, and financial and other harm.

89. The injury to Plaintiff and Class Members was a proximate, reasonably foreseeable result of Facebook's breaches of its aforementioned duties.

90. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT IV — UNJUST ENRICHMENT
(Against All Defendants)

91. Plaintiff incorporates each and every allegation above as if fully set forth herein.

92. Plaintiff and Class Members conferred a monetary benefit on Defendants in the form of Personal Information that they provided to Facebook, through the use of which Defendants obtained millions of dollars in revenue.

93. For instance, Facebook collected, maintained, and stored the Personal Information of Plaintiff and Class Members, and used this information to obtain millions of dollars in revenue.

94. Similarly, Cambridge Analytica improperly obtained the Personal Information of Plaintiff

and Class Members, and used this information to obtain millions of dollars in revenue.

95. Likewise, Doe Defendants improperly obtained the Personal Information of Plaintiff and Class Members, and used this information to obtain millions of dollars in revenue.

96. Plaintiff and Class Members also conferred a monetary benefit on Defendant Facebook by viewing and/or clicking on advertisements provided by Facebook.

97. Defendants had knowledge of the monetary benefits conferred by Plaintiff and Class Members.

98. Defendant Facebook improperly stored and failed to monitor the Personal Information with which it was entrusted by Plaintiff and Class Members, and Defendants improperly obtained and misused the Personal Information of Plaintiff and Class Members for their own benefit.

99. Defendants were therefore unjustly enriched through their improper use of Plaintiff's and Class Members' Personal Information, through which they obtained millions of dollars in revenue, in an amount to be proven at trial.

100. Because Defendants will be unjustly enriched if they are allowed to retain the revenue that they improperly obtained through the misuse of Plaintiff's and Class Members' Personal Information, Plaintiff and Class Members are entitled to recover the amount by which Defendants were unjustly enriched at their expense.

101. Accordingly, Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable amounts by which Defendants have been unjustly enriched at the expense of Plaintiff and Class Members, in addition to such other relief as this Court deems just and proper.

COUNT V — INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(Against All Defendants)

102. Plaintiff incorporates each and every allegation above as if fully set forth herein.

103. Plaintiff and Class Members reasonably expected that their Personal Information would be protected and secured from unauthorized parties and would not be disclosed to or obtained by any unauthorized parties, or disclosed or obtained for any improper purpose.

104. Defendant Facebook unlawfully invaded the privacy rights of Plaintiff and Class

Members by (a) failing to adequately secure their Personal Information from disclosure to unauthorized parties for improper purposes; (b) disclosing their Personal Information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their Personal Information to unauthorized parties without the informed and clear consent of Plaintiff and Class Members.

105. Defendant Cambridge Analytica and Doe Defendants unlawfully invaded the privacy rights of Plaintiff and Class Members by (a) wrongfully obtaining their Personal Information for improper purposes; (b) using their Personal Information for improper and unauthorized purposes, in a manner that is highly offensive to a reasonable person; (c) disclosing their Personal Information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (d) disclosing their Personal Information to unauthorized parties without the informed and clear consent of Plaintiff and Class Members.

106. Defendants thus intentionally intruded upon Plaintiff's and Class Members' solitude, seclusion, and/or private affairs, in a manner that was malicious, oppressive, and willful.

107. Defendants knew or should have known that their violations of Plaintiff's and Class Members' privacy rights would be highly offensive to a reasonable person in the same position as Plaintiff and Class Members.

108. By their actions and omissions, Defendants acted in a manner that was calculated to injure Plaintiff and Class Members, and was in conscious disregard of their privacy rights.

109. Defendants thus violated Plaintiff's and Class Members' rights to privacy under the common law as well as under state law, including but not limited to the California Constitution, Article I, Section I.

110. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' sensitive Personal Information has been viewed or is at imminent risk of being viewed by unauthorized parties, and Plaintiff's and Class Members' reasonable expectations of privacy, solitude, and seclusion have been intruded upon and frustrated. Plaintiff and Class Members have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief, including injunctive relief and punitive damages.

COUNT VI — VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
(Cal. Bus. & Prof. Code § 17200, et seq.)
(Against All Defendants)

111. Plaintiff incorporates each and every allegation above as if fully set forth herein.

112. Defendants engaged in unlawful, unfair, and fraudulent business practices in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. ("UCL").

113. The conduct alleged herein is a "business practice" within the meaning of the UCL.

114. Defendants' acts, omissions and conduct constitute unlawful, unfair, and fraudulent business practices under the UCL.

115. Defendants' acts, omissions, and conduct were unlawful, because they violated the Wiretap Act and the SCA, and because they were negligent.

116. Defendants' acts, omissions, and conduct alleged herein constitute a violation of the unlawful prong of the UCL, because Defendants failed to comport with a reasonable standard of care and public policy.

117. Defendants' acts, omissions, and conduct also constitute "unfair" business acts or practices, because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members.

118. Cambridge Analytica and Doe Defendants have engaged in fraudulent business practices by obtaining Plaintiff's and Class Members' Personal Information without authorization or in excess of authorization they, or their agents, may have obtained.

119. Facebook has engaged in fraudulent business practices by making material misrepresentations and by failing to disclose material information regarding Facebook's deficient security policies and practices, the security of Plaintiff's and Class Members' Personal Information, and by failing to provide adequate and timely notice that Plaintiff's and Class Members' Personal Information had been improperly obtained by Cambridge Analytica and Doe Defendants.

120. Facebook had exclusive knowledge of material information regarding its deficient security policies and practices, as well as regarding the security of Plaintiff's and Class Members' Personal Information.

121. Facebook also had exclusive knowledge about the misuse of Plaintiff's and Class

Members' Personal Information, including knowledge that Plaintiff's and Class Members' Personal Information had been improperly obtained by Cambridge Analytica and Doe Defendants.

122. Plaintiff and Class Members were misled by Facebook's misrepresentations and omissions about Facebook's data security, and they reasonably relied upon these misrepresentations and omissions to their detriment. But for Facebook's misrepresentations and omissions, Plaintiff and Class Members would not have provided their Personal Information to Facebook and/or would have insisted that their Personal Information be more securely protected.

123. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiff and Class Members have suffered injury in fact. Plaintiff and Class Members have been injured, in that their Personal Information has been misused and/or is at risk for imminent future misuse, including identity theft and fraud.

124. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiff and Class Members have already suffered from identity theft, identity fraud, and/or a continuing increased risk of identity theft and identity fraud due to the compromise and/or unauthorized use of their Personal Information. Plaintiff and Class Members have also been injured by, among other things: (1) the loss of the opportunity to control how their Personal Information is used; (2) the diminution in the value and/or use of their Personal Information entrusted to Facebook with the understanding that Facebook would safeguard their Personal Information against theft and not allow access and misuse of their Personal Information by others; (3) the compromise and/or misuse of their Personal Information; (4) the continued risk to their Personal Information, which remains in Facebook's possession and is subject to further misuse; and (5) costs associated with time, effort, and money that Class Members have expended or will expend, to prevent, detect, contest, and repair the impact of the Personal Information compromised as alleged herein.

125. Because of Defendants' unlawful, unfair, and fraudulent business practices, Plaintiff and Class Members are entitled to relief, including attorneys' fees and costs, restitution, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful and unfair practices. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law, including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class Members, respectfully requests that this Court:

a. Certify the Class and appoint Plaintiff as Class Representative;

b. Enter Judgment against Defendants for Plaintiff's and Class Members' asserted causes of action;

c. Award Plaintiff and Class Members appropriate relief, including actual and statutory damages, restitution, disgorgement, and punitive damages;

d. Award equitable, injunctive, and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, as well as the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal and equitable relief as this Court may find just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED this 30th day of March, 2018.

KELLER ROHRBACK L.L.P.

By /s/ *Christopher Springer*

Christopher Springer (291180)
cspringer@kellerrohrback.com
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497

Lynn Lincoln Sarko, *pro hac vice forthcoming*
Gretchen Freeman Cappio, *pro hac vice forthcoming*
Cari Campen Laufenberg, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

Attorneys for Plaintiff